DOD PRIVACY IMPACT ASSESSMENT (PIA)

1. Name of MACOM/DA Staff Proponent (APMS Sub Organization Name)

Assistant Chief of Staff for Installation Management (ACSIM), Family & Morale, Welfare and Recreation Command (F&MWRC)

2. Name of Information Technology (IT) System (APMS System Name)

Learning Management System (MWR-LMS)

3. Budget System Identification Number (SNAP-IT Initiative Number)

9990

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR))

3638

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable)

N/A

6. Privacy Act System of Records Notice Identifier (if applicable)

In Progress

7. OMB Information Collection Requirement Number (if applicable) and expiration date

N/A

8. Type of authority to collect information (statutory or otherwise).

5 U. S.C. 4101 to 4118, The Government Employees Training Action of 1958;
10 U.S.C. 3013, Secretary of the Army;
26 U.S.C. 6041, Information at Source;
E.O. 9397 (SSN);
DoD Directive 1015.2, Military Morale, Welfare and Recreation (MWR);
DoD Instruction 1015.10, Program for Military Morale, Welfare and Recreation (MWR);
Army Regulation 215-1, Morale, Welfare and Recreations Activities and Nonappropriated Fund Instrumentalities;
Army Regulation 215-3, Nonappropriated Fund Personnel Policy;
Army Regulation 215-4, Nonappropriated Fund Contracting;

Army Regulation 608-10, Child Development Services;

9. General Information: Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries, and interconnections, location of system and components, and system backup).

The Meridian KSI Learning Management System (LMS) is a computer software system providing central registration, course enrollment, web-based learning, career management and a range of performance support tools through one web portal available at http://mwraonline.com. With this tool, MWR employees can obtain training and access a range of job aids at their workstations. In addition to the opportunity to enroll in classroom courses, students have immediate access to online courses that are Sharable Content Objective Reference Model (SCORM) compliant and accessible to users regardless of their physical requirements. The LMS expands the MWR Academy's reach by providing anywhere, anytime training to employees worldwide, while reducing training costs and time away from work.

The LMS is in the Operational and Support (Sustainment) Phase of its life cycle. LMS is owned by FMWRC, Workforce Development, MWR Academy in Alexandria, VA.. The system connects to the Internet and provides client access to system services through a commercial Internet Service Provider host located at a controlled facility. LMS is located at a DOD secure facility. All hardware is government owned. Daily and weekly backups are stored internal to the system. Monthly full backup media is stored offsite in a fireproof safe to provide another level of protection by reducing the risk of an onsite disaster destroying all backups.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).

Name, social security number, e-mail address, supervisor name, employment address, duty phone and fax numbers, education level, grade, job title, length of service and installation.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

The information is collected in a web-based registration form. Active training and transcript records are maintained by the MWR Academy for seven years in order to provide students with an official transcript record. Currently, thirty MWR Academy courses are recommended for college credit by the American Council on Education (ACE).

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a DA program, etc.)

Registration profile information is collected to allow the MWR Academy to compile training statistics and maintain individual training records for DOD employees. Students activate and validate their registration through an email activation link sent to the email address they registered with.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

Site administrators use this information to compile training statistics.

14. Describe whether the system derives or creates new data about individuals through aggregation.

No, the system does not create new data about individuals when reports are run. Data is rolled up for reporting purposes based on specified query field requirements. An example may be a report that is requested on student's course completion by installation or region.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

Only site administrators and course managers have access to profile information. Identifiable information is shared only within the Component for statistical reporting purposes. Most often, social security numbers are neither required nor included in statistical reports. Course managers have a level of permissions and access to student information in order to track course enrollment/completion, and ability to notify supervisors and students regarding course requirements. Official transcripts are available to students and sent to educational institutions only at the written request of a student. Supervisor's do not have access to student enrollment or transcript information. They can obtain transcript information by requesting through their employee.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

When an individual applies for an account within the learning management system they are provided with the Privacy Act Statement. Students aren't required to complete profile information upon registration. If they do not want to participate by providing the registration data they are told to log off the system. This written notification is available on our homepage, login and registration page.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

When an individual applies for an account within the learning management system they are provided with the Privacy Act Statement on the account registration screen. Students receive system auto-generated confirmation emails upon registration and course enrollment. Upon registration, students receive their login id and password that they created, in two separate emails for security purposes. Transcripts, student certificates, course syllabi and materials are available and accessible online once the student logs into our system. Students have access only to their own transcript and certificate information. Classroom based course materials may be mailed to prospective class attendees to their work address they provided upon registration.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

MWR-LMS has passed the DITSCAP security accreditation process. The LMS is encrypted and secured through VeriSign. Permission groups restrict access to the identifiable information in the LMS. Access to data is controlled by a system administrator who is responsible for assigning access permissions beyond end user capability. A Public Key Infrastructure (PKI) certificate authority is used through a VeriSign Class 3 certificate, based on the Secure Socket Layer (SSL) protocol to protect unclassified (SI). Boundary protection devices - Protection mechanisms are implemented at the information system boundary and at layered or internal system boundaries, including, firewall, routers and network intrusion detection systems. Protection Capabilities - Controlled Release: Only traffic that is explicitly permitted (based on traffic review) is released from the boundary of the interconnected information system. Encryption- Outgoing communication, including the body and attachment of the communication, are encrypted at the appropriate level of encryption for the information, transmission medium, and destination information system for all passwords.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

A System of Records Notice is required and has been submitted to the Army Privacy Officer for approval.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form. The system and data contained in it are (classified /unclassified /sensitive /FOUO?)

Data contained in the system is unclassified, for official use only. The Privacy Impact Assessment can be published in full.